



DOCUMENT D'ACCOMPAGNEMENT DE LA CAMPAGNE NATIONALE TV-MÉDIAS DE SENSIBILISATION À LA CYBERSÉCURITÉ 2022 (CYBERMALVEILLANCE – INC)

[Cybermalveillance](#) avec l'[Institut National de la Consommation](#) (INC) dans le cadre de l'émission Consomag propose des vidéos et des outils pédagogiques sur les bonnes pratiques à adopter afin de protéger efficacement ses activités et ses appareils sur Internet.

En 2022 les thèmes portent sur le cyberharcèlement, les cyberattaques, éviter les pièges du smishing (hameçonnage par sms) et l'usurpation d'identité.

[Campagne nationale 2022 TV-médias de sensibilisation à la cybersécurité - Assistance aux victimes de cybermalveillance](#)

Les compétences numériques constituent un élément essentiel pour réussir ses études, son insertion professionnelle, et sa vie de futur citoyen dans une société dont l'environnement technologique évolue constamment, avec une utilisation réfléchie des réseaux et d'internet.

Apprendre à se servir de ces outils c'est aussi apprendre les risques de leur utilisation et comment s'en protéger.

Le domaine 5 du cadre de référence des compétences numériques (CRCN) : Protection et sécurité, évalue la capacité à l'utilisation de ses outils tout en respectant certaines règles de protection.

Les vidéos du site Cybermalveillance portent sur les comportements à adopter avec des cas concrets.

■ CYBERHARCÈLEMENT



LE LIEN AVEC LES DISCIPLINES

EDUCATION AUX MÉDIAS ET À L'INFORMATION

- Définir la notion de liberté d'expression et ses limites.
- Pouvoir se référer aux règles de base du droit d'expression et de publication, en particulier sur les réseaux.

ENSEIGNEMENT MORAL ET CIVIQUE

- Cycle 4 : « L'identité numérique » est étudiée comme composante de l'identité personnelle et légale. « Le harcèlement sur Internet et les réseaux sociaux » est également un objet d'enseignement.
- En seconde générale et technologique, l'axe 2 du programme, « Garantir les libertés, étendre les libertés : les libertés en débat » propose plusieurs objets d'enseignement parmi lesquels « Les flux informationnels et leur régulation sur internet » ; « les données numériques, traitement et protection (règlement général sur la protection des données) ».
- En première générale, l'axe 1 « Fondements et fragilités du lien social : Les nouvelles formes d'expression de la violence et de la délinquance (incivilités, cyberharcèlement, agressions physiques, phénomènes de bandes, etc.).

TECHNOLOGIE

Au cycle 4, le programme développe les compétences liées à l'utilisation des outils numériques mais travaille particulièrement sur comment adopter un comportement éthique et responsable.

SNT

En second générale et technologique un module du programme est consacré au réseau social. Les notions d'identité numérique, e-réputation, identification, authentification sont abordé. La cyberviolence est un contenu de ce module.

RESSOURCES POUR APPROFONDIR

- Article sur le cyberharcèlement du site cybermalveillance : [Que faire en cas de cyberharcèlement ou harcèlement en ligne ? - Assistance aux victimes de cybermalveillance](#)
- Le manga web réalisé par AXA avec les membres du Campus Cyber : [L'UNION FAIT LA FORCE – Cybervengers](#)

Fiches réflexes et lien avec la loi :

- <https://www.clemi.fr/fr/cles-medias/la-liberte-dexpression-et-ses-limites.html>
- <https://www.education.gouv.fr/non-au-harcelement/faire-face-au-cyberharcelement-325385>

RESSOURCES EN ACADÉMIE

Sur Édubase, une multitude de ressources sont disponibles pour travailler de ces thèmes :

- À partir du cycle 4, une ressource sur la notion d'identité numérique traitée en EMC <https://edubase.eduscol.education.fr/fiche/4569>
- En français, pour les classes de seconde professionnelle <https://pedagogie.ac-toulouse.fr/documentation/identites-numeriques-usages-traces-risques>
- En SNT, une séance sur le cyberharcèlement https://ww2.ac-poitiers.fr/doc/spip.php?article984&debut_page=2

■ CYBERATTAQUE



LE LIEN AVEC LES DISCIPLINES

ENSEIGNEMENT MORAL ET CIVIQUE

En classe de première professionnelle, le second thème « Préserver la paix et protéger des valeurs communes » est abordé par la défense et sécurité en France et en Europe. Pour exemple, « Face aux attentats terroristes, l'État se dote de nouveaux dispositifs et outils, de nouvelles instances de sécurité et de renseignement, y compris dans le domaine de la cybersécurité. »

En seconde, voie générale et technologique, l'un des objets d'enseignement proposé par le programme est « les données numériques, traitement et protection (règlement général sur la protection des données) ».

En classe terminale, voie générale et technologique, le thème annuel est « La démocratie, les démocraties » et la cybersécurité est explicitement évoquée dans l'axe 1 : « Fondements et expériences de la démocratie » : « La protection des démocraties : sécurité et défense nationales ; lutte contre le terrorisme ; état d'urgence et législation d'exception ; cybersécurité ».

NUMÉRIQUE ET SCIENCES INFORMATIQUES (ENSEIGNEMENT DE SPÉCIALITÉ – PREMIÈRE ET TERMINALE GÉNÉRALES)

Cet enseignement a vocation à développer plusieurs compétences, parmi lesquelles « faire un usage responsable et critique de l'informatique ». Une partie du programme est dédiée aux interactions entre l'homme et la machine sur le Web. La cybersécurité est un objet transversal qui peut être introduit dans les réflexions des projets des élèves.

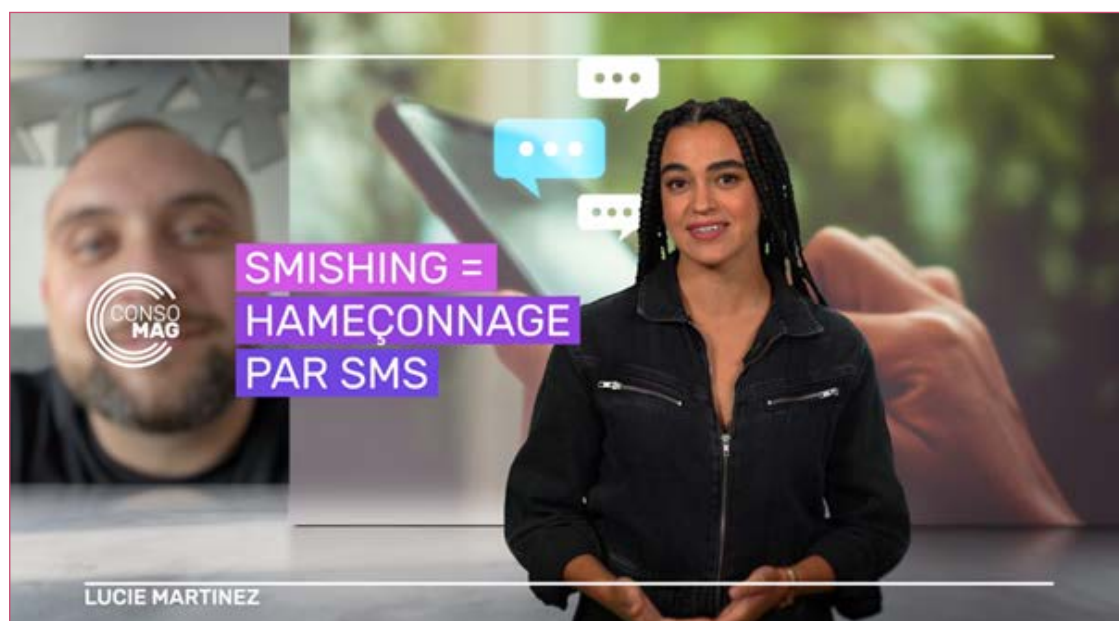
SÉRIE STMG – ENSEIGNEMENT SPÉCIFIQUE DE SYSTÈMES D'INFORMATION DE GESTION

La cybersécurité est un objet d'enseignement dans cette spécialité de la série STMG, où le programme précise : « La sécurité des systèmes d'information s'étend à la cybersécurité pour prendre en compte les événements issus du cyberspace qui sont susceptibles de compromettre la disponibilité, l'intégrité, la confidentialité ou la traçabilité des données. Cela consiste, pour l'organisation, à prévenir les actes de malveillance délibérés ou la négligence avec intention de nuire ; cela exige des techniques nouvelles comme la mise en place d'une cyberdéfense pour lutter contre la cybercriminalité. Les données font l'objet d'une protection élevée, conformément aux obligations en la matière et aux avantages stratégiques et économiques qu'elles peuvent représenter ».

RESSOURCES POUR APPROFONDIR

- L'analyse de la menace sur le site de l'ANSSI [Principales menaces | Agence nationale de la sécurité des systèmes d'information \(ssi.gouv.fr\)](https://www.ssi.gouv.fr/)
- Le manga web réalisé par AXA avec les membres du Campus Cyber : [PIRATER, N'EST PAS JOUER – Cybervengers](#)

■ SMISHING OU HAMEÇONNAGE PAR SMS : COMMENT ÉVITER LE PIÈGE ?



LE LIEN AVEC LES DISCIPLINES

Le domaine 4 « Protection et sécurité » des épreuves de Pix porte notamment sur la sécurité de l'environnement numérique : « se prémunir contre les attaques, pièges, désagréments et incidents susceptibles de nuire au bon fonctionnement des matériels, logiciels, sites internet, et de compromettre les transactions et les données ».

SNT

En classe de seconde générale et technologique, le module Web du programme, la sécurité et la confidentialité sont traités :

« En formulant des requêtes sur des sites Web dynamiques et en laissant des programmes s'exécuter sur sa machine, l'utilisateur prend des risques : il peut communiquer des informations personnelles à son insu à des serveurs qui en gardent une trace, à distance ou localement par des cookies, ou encore charger des pages contenant des programmes malveillants, par exemple permettant d'espionner en continu les actions de l'utilisateur. Par ailleurs, un navigateur peut garder un historique de toutes les interactions, et le laisser accessible aux sites connectés. L'utilisateur peut utiliser des services qui s'engagent à ne pas garder de traces de ses interactions, par exemple certains moteurs de recherche. Il peut aussi paramétrer son navigateur de façon à ce que celui-ci n'enregistre pas d'historique des interactions. De fausses pages peuvent encore être utilisées pour l'hameçonnage des utilisateurs. Un nom de lien pouvant cacher une adresse Web malveillante, il faut examiner cette adresse avant de l'activer par un clic ».

Il invite à sensibiliser les élèves aux risques liés aux cyberattaques comme l'hameçonnage.

RESSOURCES POUR APPROFONDIR

- Article sur « [Qu'est-ce que le phishing ou hameçonnage ?](#) » du site cybermalveillance
- [Arnaques par message électronique : comment identifier et déjouer l'hameçonnage](#) du site cybermalveillance
- Le manga web réalisé par AXA avec les membres du Campus Cyber : [DRAGONS ET MOUTONS – Cybervengers](#)
- [Un test](#) pour vérifier ses connaissances

■ USURPATION D'IDENTITÉ SUR INTERNET



LE LIEN AVEC LES DISCIPLINES

ENSEIGNEMENT MORAL ET CIVIQUE

Au cycle 4, « L'identité numérique » est étudiée comme composante de l'identité personnelle et légale.

PASSEPORT EDUCFI

En classe de 4ème, le passeport EDUCFI propose de sensibiliser les élèves sur l'éducation financière et budgétaire. Une partie du passeport est consacré à la sensibilisation aux arnaques comme l'hameçonnage.

SCIENCES NUMÉRIQUES ET TECHNOLOGIE (ENSEIGNEMENT DE TRONC COMMUN - SECONDE)

La partie sur les réseaux sociaux aborde l'identité numérique. Cette notion peut être réinvestie dans la partie web avec la sécurité et la confidentialité.

ÉCONOMIE-GESTION AU LYCÉE PROFESSIONNEL

En CAP, le programme précise que « L'usage régulier de l'e-communication questionne le périmètre de son utilisation : à des fins personnelles ou professionnelles, sur le lieu de travail ou ailleurs ».

En baccalauréat professionnel, dans le module 2 « La consommation : quels choix pour les ménages ? » les élèves sont amenés à savoir « Comment protéger le consommateur dans son acte d'achat ? ». Pour le e-commerce, l'élève s'interroge sur le traitement et l'utilisation des données personnelles collectées.

RESSOURCES POUR APPROFONDIR

- Article du site cybermalveillance sur l'usurpation d'identité : <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/usurpation-identite-que-faire>
- Article du site de la Banque de France sur l'usurpation d'identité : <https://particuliers.banque-france.fr/info-banque-assurance/arnaques-les-bons-reflexes/usurpation-identite-et-problemes-bancaires-que-faire>